

SEP 27 2006

In re: Brabson et al.
Serial No.: 10/007,593
Filed: December 5, 2001
Page 8 of 11

REMARKS

Applicants appreciate the continued thorough examination of the present application that is evidenced in the Official Action of July 17, 2006 (the "Official Action"). For the reasons discussed below, Applicants respectfully request reconsideration of the present application and submit that the claims, as amended, are allowable over the art of record.

Status of the Claims

Claims 1-6, 9-23, 25 and 26 are pending in the present application. Claims 1, 18, 21, and 25-26 stand rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 6,070,198 to Krause et al. ("Krause"). Claims 2-6, 9-17, 19, and 22-23 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Krause in view of Mod_SSL manual. Claim 20 stands rejected as unpatentable under 35 U.S.C. § 103(a) over Krause in view of U.S. Patent No. 6,801,927 to Smith et al. ("Smith").

Claim Amendments

Claim 1 has been amended to clarify that selectably securing the at least one communication of the executing application program is performed in response to the invocation of the at least one security directive. Corresponding amendments have been made to Claims 25 and 26. Claims 10 and 11 have been amended to correct the dependency error noted in the Office Action.

The Independent Claims Are Patentable Over the Cited References

Applicants submit that Claim 1, as amended, is patentable over Krause. Claim 1 has been amended to clarify that selectably securing the at least one communication of the executing application program is performed in response to the invocation of the at least one security directive. In particular, Claim 1, as amended, recites:

1. A method of improving security processing in a computing network, comprising:
providing security processing in an operating system kernel;

In re: Brabson et al.
Serial No.: 10/007,593
Filed: December 5, 2001
Page 9 of 11

providing an application program which makes use of the operating system kernel during execution;
executing the application program;
selectably securing at least one communication of the executing application program with a remotely executing application program using the provided security processing in the operating system kernel;
providing, in the security processing, support for at least one security directive;
and
invoking, during execution of the provided application program, the at least one security directive, wherein selectably securing the at least one communication of the executing application program is performed in response to the invocation of the at least one security directive.

The invention of Claim 1 provides an application that has some secure socket layer (SSL) awareness with an ability to utilize kernel-based security processing functionality by invoking a security directive for which support has been provided in the security processing. Thus, an application may invoke kernel-based security processing with only a minimal amount of security processing awareness added to the application itself. *See*, Specification, page 7, ll. 16-18.

The Official Action asserts that the modified `ifconfig` function call discussed at col. 6, ll. 26-41 of Krause constitutes a security directive as described above. As noted by Krause, the `ifconfig` command is a Unix administrative command used to configure network addresses. That is, the Unix `ifconfig` command is not an api function call, such as a `send()` or `copyin()` function that may be invoked by an executing application program. While the `ifconfig` command may be used by a system administrator to define encryption parameters of a network connection, it is in the nature of a system configuration command, not a security directive that may be invoked by an executing application program.

Furthermore, Krause does not disclose that an application program invokes the `ifconfig` function to selectably secure a communication of the application program, as recited in Claim 1. Instead, as noted in the Office Action at page 6, the application program invokes a system call, such as a `send()` command. While security processing is performed on the data sent by the application program, the application program itself is not invoking a security directive, as recited in Claim 1. Moreover, in the system of Krause, a communication of an application program is

In re: Brabson et al.
Serial No.: 10/007,593
Filed: December 5, 2001
Page 10 of 11

not selectably secured in response to a security directive invoked during execution of the application program, as recited in Claim 1.

The system of Krause performs security processing for application programs without providing support for security directives that may be invoked by the executing application programs. Therefore, in contrast to claim 1 in which an application may explicitly invoke a security directive to trigger kernel-based security processing, an application program running in the system of Krause has no control over whether or not security processing is performed on a communication of the application program. Thus, Applicants respectfully submit that Claim 1, as amended, is patentable over Krause.

Claims 25-26 include similar recitations as Claim 1, and accordingly are patentable for at least these reasons.

The Dependent Claims Are Patentable Over the Cited References

The dependent claims are patentable at least as per the patentability of Claim 1. In addition, many of the dependent claims are separately patentable. For example, Claim 12 recites providing, in the secure processing, support for a security directive that requests selectably securing the at least one communication of the executing application program to begin operating. Similarly, Claim 13 recites providing, in the secure processing, support for a security directive that requests selectably securing the at least one communication of the executing application program to stop operating. As noted above, the system of Krause performs security processing for application programs without providing support for security directives that may be invoked by the executing application programs. In contrast, in a system configured to perform a method according to Claims 12 and/or 13, an application having SSL awareness may control some aspects of security processing, such as starting and/or stopping the security processing. *See*, Specification, p. 16, ll. 17-19. Thus, Claims 12 and 13 are patentable for at least these additional reasons.

In re: Brabson et al.
Serial No.: 10/007,593
Filed: December 5, 2001
Page 11 of 11

RECEIVED
CENTRAL FAX CENTER

SEP 27 2006

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,



David C. Hall
Registration No. 38,904
Attorney for Applicants

Customer Number 46589
Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)